فصلنامه طلوع نگارندگان عدالت
www.journaltne.ir

مسئولیت بین‌المللی دولت‌ها در قبال حملات سایبری به زیرساخت‌های حیاتی: چالش‌های انتساب و استانداردهای اثباتی

علیرضا انصاری مهیاری[۱]،فروغ قاسمیان هفشجانی[۲]

چکیده

حملات سایبری به زیرساخت‌های حیاتی کشورها در دو دهه اخیر به یکی از مهم‌ترین چالش‌های حقوق بین‌الملل تبدیل شده است. این مقاله با رویکردی تحلیلی–حقوقی به بررسی مسئولیت بین‌المللی دولت‌ها در قبال حملات سایبری به زیرساخت‌های حیاتی می‌پردازد و بر دو مانع اساسی در این زمینه تمرکز دارد: دشواری اثبات انتساب حملات به دولت‌ها به دلیل ماهیت ناملموس و فرامرزی فضای سایبر، و عدم وجود استانداردهای روشن و یکسان درباره سطح ادله مورد نیاز برای اثبات حملات سایبری. بررسی رویه دولت‌ها در مواردی مانند استاکس‌نت و حملات به زیرساخت‌های اوکراین نشان می‌دهد که دولت‌ها اغلب از پذیرش مسئولیت خودداری کرده و راهبرد انکار را در پیش می‌گیرند. یافته‌های پژوهش نشان می‌دهد که اصل مراقبت بایسته که در قضیه تنگه کورفو توسط دیوان بین‌المللی دادگستری به رسمیت شناخته شده است، می‌تواند مبنایی برای مسئولیت دولت‌ها در قبال حملات سایبری از قلمرو خود فراهم آورد. با این حال، چالش‌های اثباتی و فقدان رویه قضایی مشخص، کاربست این قواعد را با دشواری مواجه ساخته است و ضرورت تدوین قواعد روشن‌تر در این زمینه را آشکار می‌سازد.

واژگان کلیدی :مسئولیت بین‌المللی دولت‌ها، حملات سایبری، زیرساخت‌های حیاتی، انتساب، مراقبت بایسته، استانداردهای اثباتی.

[۱] استادیارگروه حقوق،واحدنجف آباد،دانشگاه آزاد اسلامی،نجف آباد،ایران.

[۲] دانشجوی دکتری حقوق بین الملل، واحد نجف آباد، دانشگاه ازاد اسلامی، نجف آباد، ایران. behnaz.jahanbazi@iau.ac.ir

فصلنامه طلوع نگارندگان عدالت
www.journaltne.ir

مقدمه

حملات سایبری به زیرساخت‌های حیاتی کشورها در دو دهه اخیر به یکی از مهم‌ترین چالش‌های حقوق بین‌الملل تبدیل شده است. زیرساخت‌های حیاتی شامل تأسیسات انرژی، شبکه‌های آب و برق، سیستم‌های حمل‌ونقل، بیمارستان‌ها و سیستم‌های مالی هستند که اختلال در عملکرد هر یک می‌تواند پیامدهای فاجعه‌باری برای جوامع به دنبال داشته باشد (حیدری‌فرد، ۱٤۰۰: ۱٥٦). حملات سایبری به این زیرساخت‌ها نه‌تنها می‌تواند موجب خسارات اقتصادی گسترده شود، بلکه در مواردی می‌تواند به تلفات جانی و نقض حقوق بشر منجر گردد (بشیری، ۱۳۹٤: ۲). با این حال، تعیین مسئولیت بین‌المللی دولت‌ها در قبال چنین حملاتی با چالش‌های حقوقی و فنی متعددی مواجه است که از جمله مهم‌ترین آنها می‌توان به دشواری انتساب و فقدان استانداردهای اثباتی روشن اشاره کرد.

مهم‌ترین چالش فراروی این موضوع، مسئله انتساب (Attribution) است. برای تحقق مسئولیت بین‌المللی یک دولت در قبال یک حمله سایبری، باید اثبات شود که آن حمله قابل انتساب به آن دولت است (قرشی سروندانی، ۱۳۹۱: ٤٥). با این حال، ویژگی‌های خاص فضای سایبر مانند ناشناس بودن، قابلیت جعل و سرعت و پیچیدگی حملات، فرآیند انتساب را با دشواری‌های بی‌سابقه‌ای مواجه ساخته است (کولین، ۲۰۱۳: ٦۰). مهاجمان سایبری می‌توانند با استفاده از ابزارهایی مانند پروکسی، شبکه‌های Tor و سرورهای زنجیره‌ای، هویت واقعی خود را پنهان کنند و یا آثاری از خود بر جای بگذارند که به دولت دیگری نسبت داده شود. این ویژگی‌ها، امکان انکار معقول را برای دولت‌ها فراهم می‌آورد و کاربست قواعد سنتی مسئولیت دولت‌ها را با چالش مواجه می‌سازد (امیری و حیدری‌فرد، ۱۳۹۷: ۱٥۸).

چالش دوم، فقدان استانداردهای روشن و یکسان درباره سطح ادله مورد نیاز برای اثبات حملات سایبری است. در حالی که در حوزه‌های سنتی حقوق بین‌الملل، معیارهای اثباتی نسبتاً روشنی وجود دارد، در حوزه حملات سایبری، جامعه بین‌الملل هنوز به اجماعی در این زمینه دست نیافته است (اصلانی و رنجبریان، ۱۳۹٤: ۲٦۰). برخی از دولت‌ها معیارهای اثباتی سخت‌گیرانه‌تری را طلب می‌کنند، در حالی که برخی دیگر با معیارهای انعطاف‌پذیرتر موافق هستند. این عدم اجماع، به دولت‌ها امکان می‌دهد تا از مسئولیت‌پذیری در قبال حملات سایبری فرار کنند و پاسخ‌گویی را با دشواری مواجه سازد.

اهمیت بررسی این موضوع از آن جهت است که زیرساخت‌های حیاتی کشورها به‌طور فزاینده‌ای در معرض تهدیدات سایبری قرار دارند و اختلال در عملکرد آنها می‌تولند پیامدهای جبران‌ناپذیری برای امنیت ملی و رفاه عمومی داشته باشد. حملات سایبری به زیرساخت‌های حیاتی، از معضلات نوین حقوق بین‌الملل محسوب می‌شود که نسبت به آن‌ها هیچ گونه قاعده‌ای در سطح بین‌المللی وضع نگردیده است (بشیری، ۱۳۹٤: ۱). با این حال، با بررسی این حملات بر اساس چهارچوب‌های سنتی حقوق بین‌الملل می‌توان این گونه نتیجه گرفت که

فصلنامه طلوع نگارندگان عدالت
www.journaltne.ir

سطح قابل‌توجهی از این حملات موجب نقض اصل عدم توسل به زور، اصل عدم مداخله و اصل برابری دولت‌ها بوده است (بشیری، ۱۳۹٤: ۱). بدافزار استاکس‌نت که در سال ۲۰۱۰ تأسیسات هسته‌ای ایران را هدف قرار داد، نقطه عطفی در این بحث محسوب می‌شود و بسیاری از حقوقدانان آن را با یک حمله مسلحانه قابل مقایسه دانسته‌اند (نامدار و قاسمی، ۱۳۹۷: ۲۱۰). این حمله نشان داد که حملات سایبری می‌توانند به‌اندازه حملات نظامی سنتی، خسارت‌بار و مؤثر باشند و از این رو، به عنوان یک ابزار راهبردی در منازعات بین‌المللی مورد توجه قرار گرفتند.

ساختار مقاله بدین گونه است که در بخش نخست به بررسی مبانی مسئولیت بین‌المللی دولت‌ها در حقوق بین‌الملل و قواعد عمومی حاکم بر آن پرداخته می‌شود. در بخش دوم، چالش‌های انتساب حملات سایبری به دولت‌ها با تأکید بر معیارهای کنترل مؤثر و کنترل کلی و نیز اصل مراقبت بایسته تحلیل می‌گردد. در بخش سوم، استانداردهای اثباتی در حملات سایبری و رویه دولت‌ها در این زمینه مورد بررسی قرار می‌گیرد. در بخش چهارم، مطالعه موردی حملات سایبری به زیرساخت‌های حیاتی شامل استاکس‌نت و حملات به زیرساخت‌های اوکراین و ایران تحلیل می‌شود. در نهایت، نتیجه‌گیری و پیشنهادات ارائه می‌گردد.

۱- مبانی مسئولیت بین‌المللی دولت‌ها در قبال حملات سایبری

۱-۱.قواعد عمومی مسئولیت دولت‌ها

مسئولیت بین‌المللی دولت‌ها یکی از بنیادین‌ترین موضوعات حقوق بین‌الملل است که به تعیین آثار حقوقی ناشی از نقض تعهدات بین‌المللی توسط دولت‌ها می‌پردازد. طرح مواد راجع به مسئولیت دولت‌ها در قبال اعمال متخلفانه بین‌المللی (ARSIWA) که توسط کمیسیون حقوق بین‌الملل تدوین شده است، چارچوب اصلی این حوزه را تشکیل می‌دهد. بر اساس این طرح، هر رفتار متخلفانه بین‌المللی یک دولت، شامل دو عنصر اساسی است: نخست، اینکه رفتار مذکور قابل انتساب به آن دولت باشد و دوم، اینکه آن رفتار، تعهد بین‌المللی آن دولت را نقض کند (ILC, ۲۰۰۱: Art. ۲).این دو شرط، به‌عنوان پیش‌شرط‌های اساسی برای تحقق مسئولیت بین‌المللی دولت‌ها محسوب می‌شوند و در صورت عدم احراز هر یک، مسئولیتی برای دولت متصور نخواهد بود.

ماده ٤ این طرح، رفتار ارکان دولت از جمله قوه مقننه، مجریه و قضائیه را به‌طور مستقیم به دولت قابل انتساب می‌داند. ماده ۵ نیز رفتار اشخاص یا نهادهایی را که اگرچه رکن رسمی دولت نیستند، اما به موجب قانون دولت، صلاحیت اعمال اقتدار عمومی را دارند، قابل انتساب به دولت می‌داند (حلمی، ۱۳۸۷: ۱۲۰). ماده ٦ رفتار ارکانی را که در اختیار دولت دیگر قرار گرفته‌اند، به دولت پذیرنده قابل انتساب می‌داند و ماده ۷ بر انتساب رفتار ارکان یا اشخاصی تأکید دارد که فراتر از اختیارات خود یا برخلاف دستورالعمل‌ها عمل می‌کنند، مشروط بر اینکه در مقام رسمی خود عمل کرده باشند (حلمی، ۱۳۸۷: ۱۲۵). با این حال، مهم‌ترین ماده در خصوص گروه‌های غیردولتی که در حملات سایبری نقش کلیدی ایفا می‌کنند، ماده ۸ است که مقرر می‌دارد رفتار یک شخص یا گروه از اشخاص،

فصلنامه طلوع نگارندگان عدالت
www.journaltne.ir

در صورتی به‌عنوان رفتار یک دولت در حقوق بین‌الملل تلقی می‌شود که آن شخص یا گروه در واقع بر اساس دستورات یا به هدایت یا تحت کنترل آن دولت عمل کند.(ILC, ۲۰۰۱: Art. ۸)

مواد ۹ تا ۱۱ طرح نیز به سایر موارد انتساب می‌پردازند. ماده ۹، رفتار اشخاص یا گروه‌هایی را که در غیاب یا فقدان ارکان رسمی دولت، اقدام به اعمال اقتدار عمومی می‌کنند، قابل انتساب به دولت می‌داند. ماده ۱۰ به انتساب رفتار جنبش‌های شورشی یا انقلابی می‌پردازد که در صورت موفقیت، اعمال آنها به دولت جدید قابل انتساب خواهد بود. ماده ۱۱ که از اهمیت ویژه‌ای در بحث حملات سایبری برخوردار است، به موضوع پذیرش و تأیید رفتار توسط دولت می‌پردازد و مقرر می‌دارد که رفتاری که به موجب مواد ٤ تا ۱۰ قابل انتساب نیست، در صورتی به دولت قابل انتساب خواهد بود که آن دولت، آن رفتار را به‌عنوان رفتار خود تأیید و پذیرش کند :(ILC, ۲۰۰۱ .(Art. ۱۱این ماده می‌تواند در مواردی که دولتی پس از وقوع یک حمله سایبری توسط یک گروه غیردولتی، از آن حمایت یا آن را تأیید کند، مبنای مسئولیت قرار گیرد، هرچند اثبات این تأیید نیز در عمل با دشواری‌هایی مواجه است (نصیری محلاتی، ۱۳۸۹: ٦۰).

در صورت تحقق مسئولیت بین‌المللی، آثار حقوقی آن شامل سه دسته اصلی است: نخست، تعهد به توقف عمل متخلفانه و تضمین عدم تکرار آن(ILC, ۲۰۰۱: Art. ۳۰) ؛ دوم، تعهد به جبران کامل خسارت واردشده که می‌تواند به‌صورت اعاده وضع به حالت سابق، جبران خسارت مادی یا رضایت‌خواهی باشد .(ILC, ۲۰۰۱: Art. ۳۱-۳۷)؛ و سوم، حق دولت زیان‌دیده برای اتخاذ اقدامات متقابل علیه دولت متخلف، مشروط بر رعایت شرایط قانونی از جمله تناسب و موقتی بودن .(ILC, ۲۰۰۱: Art. ٤۹-٥۳) با این حال، در حوزه حملات سایبری، اعمال این آثار با چالش‌های جدی مواجه است. به‌عنوان مثال، توقف عمل متخلفانه در حملات سایبری ممکن است به دلیل عدم شناسایی دقیق عاملان یا ادامه حملات از طریق گروه‌های نیابتی، دشوار باشد. همچنین، جبران خسارت در حملات سایبری به دلیل ماهیت ناملموس برخی از خسارت‌ها و دشواری در تعیین میزان دقیق آنها، با پیچیدگی‌های فراوانی مواجه است.

۱-۲.زیرساخت‌های حیاتی و حمایت از آنها در حقوق بین‌الملل

زیرساخت‌های حیاتی به مجموعه تأسیسات، شبکه‌ها و سیستم‌هایی اطلاق می‌شوند که عملکرد آنها برای ادامه حیات اقتصادی، اجتماعی و امنیتی یک کشور ضروری است. این زیرساخت‌ها شامل بخش‌های انرژی، آب، حمل‌ونقل، ارتباطات، بهداشت و درمان، مالی و بانکی، و خدمات اضطراری می‌شوند (حیدری‌فرد، ۱٤۰۰: ۱٥۸). در حقوق بین‌الملل بشردوستانه، حمایت از زیرساخت‌های حیاتی در مخاصمات مسلحانه، به‌ویژه تأسیسات حاوی نیروهای خطرناک مانند سدها و نیروگاه‌های هسته‌ای، مورد توجه قرار گرفته است. پروتکل اول الحاقی به کنوانسیون‌های ژنو (۱۹۷۷)، در ماده ٥٦ خود، حمایت ویژه‌ای از تأسیسات حاوی نیروهای خطرناک به عمل آورده

فصلنامه طلوع نگارندگان عدالت
www.journaltne.ir

و حملات به آنها را حتی در صورت داشتن هدف نظامی، در صورتی که موجب تلفات جانی گسترده شود، ممنوع کرده است (حیدری‌فرد، ۱٤۰۰: ۱٦۰).

افزایش روزافزون سطح اتکای عملکرد بسیاری از زیرساخت‌های شهری به فضای مجازی، هشدارها نسبت به آسیب‌پذیری آنها را به دنبال داشته است (حیدری‌فرد، ۱٤۰۰: ۱٥٦). بخصوص وقتی که بدانیم ترتیبات قراردادی این حوزه حقوقی بر مبنای شرایط عینی بروز جنگ‌های کلاسیک تدوین شده‌اند و تفاوت‌های ماهوی آن با نبرد سایبری، طبیعتاً چالش‌های اساسی در اعمال قواعد هدایت مخاصمات در این عرصه را باعث می‌گردد (حیدری‌فرد، ۱٤۰۰: ۱٥۷). حملات سایبری به زیرساخت‌های حیاتی، به دلیل اینکه اغلب در زمان صلح و توسط بازیگران غیردولتی انجام می‌شوند، به‌ندرت در چارچوب قواعد حقوق بشردوستانه قابل تحلیل هستند و لذا، نیازمند چارچوب حقوقی دیگری هستند که بتواند پاسخگوی این نوع تهدیدات باشد.

از این رو، قواعد عمومی حقوق بین‌الملل از جمله اصل ممنوعیت توسل به زور، اصل عدم مداخله و قواعد مسئولیت دولت‌ها، می‌توانند مبنایی برای حمایت از زیرساخت‌های حیاتی در برابر حملات سایبری فراهم آورند. اصل ممنوعیت توسل به زور که در ماده ۲ بند ٤ منشور ملل متحد تجلی یافته است، دولت‌ها را از تهدید به زور یا استفاده از زور علیه تمامیت ارضی یا استقلال سیاسی یکدیگر منع می‌کند (ضیایی بیگدلی، ۱۳۸٤: ۱۸۰). اصل عدم مداخله نیز دولت‌ها را از دخالت در امور داخلی یکدیگر بازمی‌دارد. حملات سایبری به زیرساخت‌های حیاتی که منجر به اختلال در عملکرد آنها می‌شود، می‌تواند مصداق نقض هر دو اصل مذکور محسوب شود، به‌ویژه اگر با هدف تضعیف اقتصادی، سیاسی یا اجتماعی دولت هدف انجام شود (بشیری، ۱۳۹٤: ۳).

۱-۳.خلأ هنجاری در حمایت از زیرساخت‌های حیاتی در برابر حملات سایبری

با وجود اهمیت روزافزون زیرساخت‌های حیاتی و افزایش تهدیدات سایبری متوجه آنها، حقوق بین‌الملل موجود با خلأ هنجاری قابل‌توجهی در این زمینه مواجه است. در حالی که در سطح داخلی، بسیاری از دولت‌ها قوانین و مقررات خاصی برای حفاظت از زیرساخت‌های حیاتی خود وضع کرده‌اند، در سطح بین‌المللی، هیچ معاهده جامعی در این زمینه وجود ندارد (اصلانی و رنجبریان، ۱۳۹٤: ۲۷۵). تلاش‌های برخی کشورها و مجامع بین‌المللی برای نظام‌مندسازی ابزارها، شیوه‌ها و اثرات حملات سایبری، هنوز با توجه به عدم اجماع و وفاق جامعه جهانی منتهی به یک سند بین‌المللی نشده است (امیری و حیدری‌فرد، ۱۳۹۷: ۱۷۵). این خلأ هنجاری، به دولت‌ها امکان می‌دهد تا با بهره‌گیری از ابهامات حقوقی، به اعمال راهبردهای خصمانه در فضای سایبر بپردازند و از مسئولیت بین‌المللی فرار کنند.

یکی از موانع اصلی تدوین قواعد بین‌المللی در این زمینه، عدم اجماع بر سر تعریف «حمله سایبری» و تعیین اینکه چه نوع حملاتی می‌توانند مصداق «توسل به زور» یا «حمله مسلحانه» محسوب شوند، است (اصلانی و رنجبریان، ۱۳۹٤: ۲۵۸). این عدم اجماع، کاربست قواعد موجود را با دشواری مواجه ساخته و دولت‌ها را در مواجهه با حملات سایبری به زیرساخت‌های خود، در موقعیتی نامطمئن قرار داده است. برخی از دولت‌ها، حمله سایبری را

فصلنامه طلوع نگارندگان عدالت
www.journaltne.ir

در چارچوب عملیات اطلاعاتی و برخی دیگر به‌عنوان یک اقدام نظامی تلقی می‌کنند و این اختلاف نظر، فرآیند تشخیص مصداق و تعیین واکنش مناسب را با دشواری مواجه می‌سازد (اصلانی و رنجبریان، ۱۳۹٤: ۲٦۰).

دستورالعمل تالین که توسط گروهی از کارشناسان بین‌المللی تدوین شده است، تلاش کرده تا با ارائه معیارهایی مانند «شدت»، «آثار فوری»، «نفوذ نظامی» و «ماهیت ابزارهای به‌کاررفته»، به این ابهامات پاسخ دهد (Schmitt, ۲۰۱۳: ٤٥). با این حال، این دستورالعمل از اعتبار حقوقی الزام‌آور برخوردار نیست و صرفاً به‌عنوان یک منبع دکترینال قابل استناد است. همچنین، این دستورالعمل عمدتاً بر حملات سایبری در چارچوب مخاصمات مسلحانه متمرکز است و به حملات سایبری در زمان صلح که زیرساخت‌های حیاتی را هدف قرار می‌دهند، کمتر پرداخته است (محمدعلی‌پور، ۱۳۹۷: ۲٤٥). با توجه به این خلأها، ضرورت تدوین قواعد روشن‌تر و جامع‌تری که بتواند حمایت از زیرساخت‌های حیاتی را در برابر حملات سایبری در تمامی شرایط تضمین کند، بیش از پیش احساس می‌شود.

۲- چالش‌های انتساب حملات سایبری به دولت‌ها

۲-۱. معیار کنترل مؤثر و کارایی آن در حملات سایبری

دیوان بین‌المللی دادگستری در پرونده نیکاراگوئه (۱۹۸٦)، معیار «کنترل مؤثر» را به‌عنوان شرط انتساب رفتار گروه‌های غیردولتی به دولت تعیین کرد. دیوان در این رأی تصریح کرد که برای احراز مسئولیت حقوقی دولت، باید اثبات شود که آن دولت کنترل مؤثر بر عملیات نظامی یا شبه‌نظامی داشته است که در جریان آنها نقض‌های ادعایی رخ داده است (ICJ, ۱۹۸٦: para. ۱۱٥). به بیان دقیق‌تر، دیوان اعلام کرد که مشارکت ایالات متحده، حتی اگر در تأمین مالی، سازمان‌دهی، آموزش، تأمین تجهیزات و برنامه‌ریزی عملیات کنتراها تعیین‌کننده یا حتی قاطع بوده باشد، به‌تنهایی برای انتساب اعمال کنتراها به ایالات متحده کافی نیست (راعی، ۱۳۸۸: ۱٥٤). دیوان همچنین تأکید کرد که همه اشکال مشارکت و حتی کنترل عمومی بر گروهی از اشخاص که به نفع یک دولت دست به اعمال خلاف می‌زنند، به خودی خود، به معنای کنترل یا هدایت اعمال خاص موردنظر نیست.

این معیار در پرونده نسل‌کشی بوسنی (۲۰۰۷) نیز مورد تأکید مجدد قرار گرفت. دیوان در آن پرونده، استاندارد «کنترل کلی» را رد کرد و مجدداً بر لزوم اثبات کنترل مؤثر تأکید نمود (ICJ, ۲۰۰۷: para. ٤۰۳). دیوان در این رأی، استدلال کرد که معیار کنترل کلی، سطح اثباتی بسیار پایینی دارد و ممکن است به انتساب نادرست رفتار به دولت‌ها و نقض حاکمیت آنها منجر شود. بررسی رویه دیوان بین‌المللی دادگستری نشان می‌دهد دیوان در خصوص ضابطه کنترل در قضایای مختلف رویه‌ای واحد پیموده و در رویارویی با چالش‌های رویه خود توسط سایر مراجع حل‌وفصل اختلاف، بر رویه خود تاکید کرده است (ملکی‌زاده، ۱۳۹۲: ۱٦۰). با این حال، برخی از صاحبنظران بر این باورند که رویه دیوان در این زمینه چندان شفاف نیست و ابهامات زیادی در مورد نحوه احراز کنترل مؤثر وجود دارد (راعی، ۱۳۸۸: ۱٥٦).

فصلنامه طلوع نگارندگان عدالت
www.journaltne.ir

با این حال، در فضـای سـایبر، اثبات کنترل مؤثر بر گروه‌های هکری که ماهیتی پراکنده و غیرمتمرکز دارند، تقریباً ناممکن است. به‌ویژه اینکه گروه‌های هکری معمولاً فاقد ساختار سلسله‌مراتبی هستند و اعضای آنها ممکن است در کشورهای مختلف زندگی کنند و به‌صورت مستقل و خودجوش عمل کنند (قرشی سروندانی، ۱۳۹۱: ۷۸). در چنین شـرایطی، اثبات اینکه یک دولت خاص، کنترل مؤثر بر عملیات خاص یک گروه هکری داشـته اسـت، کاری بس دشوار و گاه غیرممکن خواهد بود. مهاجمان سایبری می‌توانند با استفاده از ابزارهای فنی پیشرفته، ردپای خود را پاک کنند و هرگونه ارتباط با دولت را مخفی سـازند (کولین، ۲۰۱۳: ٦٥). همچنین، دولت‌ها می‌توانند از شرکت‌های امنیتی خصوصی یا پیمانکاران نظامی برای انجام عملیات سایبری استفاده کنند و بدین‌ترتیب، مسئولیت خود را با لایه‌های مختلف واسطه پنهان سازند. با توجه به این موانع، به نظر می‌رسد که معیار کنترل مؤثر، به‌تنهایی نمی‌تواند مبنای مناسبی برای انتساب حملات سایبری به دولت‌ها باشد و نیازمند تکمیل با معیارهای دیگر است.

۲-۲.معیار کنترل کلی و جایگاه آن در فضای سایبر

معیار «کنترل کلی» که توسط دادگاه کیفری بین‌المللی برای یوگسـلاوی سـابق در پرونده تادیچ (۱۹۹۹) ارائه شـد، رویکردی گسترده‌تر نسبت به کنترل مؤثر دارد. بر اساس این معیار، برای انتساب رفتار گروه‌های غیردولتی به یک دولت، اثبات کنترل کلی دولت بر گروه مذکور کافی اسـت و نیازی به اثبات کنترل بر هر عمل خاصـی نیسـت (راعی، ۱۳۸۸: ۱۵۸). به عبارت دیگر، دولت باید نقش سـازمان‌دهنده، هماهنگ‌کننده یا پشـتیبان عملیات نظامی گروه را داشـته باشـد، نه فقط تأمین‌کننده تجهیزات و بودجه. دادگاه اسـتدلال کرد که در شـرایطی که یک گروه شبه‌نظامی کاملاً به یک دولت وابسته است و آن دولت، نقش تعیین‌کننده در سازماندهی، تأمین مالی و برنامه‌ریزی عملیات آن دارد، می‌توان اعضای آن گروه را به‌عنوان ارکان دفاکتو یا نمایندگان واقعی آن دولت تلقی کرد.

اتخاذ رویه‌های گوناگون از سوی مراجع قضایی بین‌المللی در زمینه ضـابطه کنترل، نشـان از تعارض رویه قضـایی بین‌المللی در این موضوع است و دیوان در قضیه نیکاراگوا و نسل‌زدایی، معیارهای مربوط به کنترل را مورد بررسی قرار داد، در حالی که دادگاه کیفری بین‌المللی یوگسـلاوی سـابق به شـیوه‌ای متفاوت به ضـابطه کنترل توجه کرد (ملکی‌زاده، ۱۳۹۲: ۱٦۲). ضـابطه کنترل مؤثر در زمینه مسئولیت بین‌المللی قابل طرح اسـت، اما ضـابطه کنترل کلی در موضوع رسیدگی به مسئولیت کیفری افراد موضوعیت پیدا می‌کند (ملکی‌زاده، ۱۳۹۲: ۱٦۳). با این حال، دیوان بین‌المللی دادگستری در رأی خود در پرونده نسل‌کشی بوسنی، به‌صراحت این معیار را به دلیل سطح پایین اثباتی که ارائه می‌دهد و احتمال نقض حاکمیت دولت‌ها رد کرد.(ICJ, ۲۰۰۷: para. ٤۰۳)

با وجود این، در فضای سایبر که اثبات کنترل مؤثر بر گروه‌های هکری بسیار دشوار است، برخی از صاحبنظران بر این باورند که معیار کنترل کلی می‌تواند کارآمدتر باشـد (کولین، ۲۰۱۳: ۷۵). این گروه اسـتدلال می‌کنند که در فضای سایبر، دولت‌ها معمولاً به‌جای صدور دستورات مستقیم، به حمایت مالی، تأمین تجهیزات و ارائه اطلاعات به گروه‌های هکری می‌پردازند و این نوع حمایت، بیشتر با معیار کنترل کلی سازگار است. با این حال، این دیدگاه نیز با انتقادهایی مواجه است، از جمله اینکه پذیرش معیار کنترل کلی، ممکن است به سوءاستفاده‌های سیاسی و

فصلنامه طلوع نگارندگان عدالت
www.journaltne.ir

انتساب‌های بی‌اساس منجر شود و حاکمیت دولت‌ها را تضعیف کند (محمدعلی‌پور، ۱۳۹۷: ۲۵۰). با توجه به این ملاحظات، به نظر می‌رسد که معیار کنترل کلی نیز به‌تنهایی نمی‌تواند پاسخگوی چالش‌های انتساب در فضای سایبر باشد و نیازمند رویکردی ترکیبی است که هم ابعاد حقوقی و هم واقعیت‌های فنی فضای سایبر را در نظر بگیرد.

۲-۳.اصل مراقبت بایسته؛ راهکاری عملی در فضای سایبر

علاوه بر معیارهای کنترل مؤثر و کنترل کلی، قاعده دیگری نیز در حقوق بین‌الملل وجود دارد که می‌تواند مبنای مسئولیت دولت‌ها در قبال حملات سایبری به زیرساخت‌های حیاتی قرار گیرد. اصل مراقبت بایسته (Due Diligence)، دولت‌ها را ملزم می‌کند که از اقدامات مخربی که از قلمرو آن دولت سرچشمه می‌گیرد و به حقوق دولت‌های دیگر آسیب می‌رساند، جلوگیری کنند (حدادی و مرادیان، ۱۳۹۸: ۱۶۸). بر اساس این اصل، دولت موظف است با استفاده از ابزارهای مناسب، از وقوع اعمال متخلفانه توسط اشخاص خصوصی در قلمرو خود جلوگیری کند (حدادی و مرادیان، ۱۳۹۸: ۱۷۰). این اصل در قضیه تنگه کورفو (۱۹۴۹) توسط دیوان بین‌المللی دادگستری به رسمیت شناخته شد و دیوان اعلام داشت که هر دولتی موظف است اجازه ندهد قلمرو آن برای اقدامات خلاف حقوق دولت‌های دیگر مورد استفاده قرار گیرد.(ICJ, ۱۹۴۹: ۲۲)

مراقبت بایسته به معنای هوشیاری لازم در انجام تعهد حقوقی، یکی از اصول حقوق بین‌الملل است که بارها در دیوان‌های بین‌المللی تایید شده است (حدادی و مرادیان، ۱۳۹۸: ۱۶۶). علاوه بر زمینه‌های عرفی الزامات این اصل، کشورها آن را در معاهدات بسیاری وارد نموده و در چارچوب تعهدات قراردادی نیز سامان داده‌اند (حدادی و مرادیان، ۱۳۹۸: ۱۷۵). یکی از نمونه‌های بارز این اصل در حوزه مبارزه با تأمین مالی تروریسم، الزامات گروه ویژه اقدام مالی (FATF) است که دولت‌ها را به اعمال نظارت بر سیستم‌های مالی و جلوگیری از سوءاستفاده آنها توسط تروریست‌ها ملزم می‌کند (حدادی و مرادیان، ۱۳۹۸: ۱۸۰). این اصل در حوزه فضای سایبر نیز مورد توجه قرار گرفته است و دستورالعمل تالین، در قاعده ٦ خود، به اصل مراقبت بایسته در فضای سایبر اشاره کرده است (Schmitt, ۲۰۱۳: ۳۱).

به‌کارگیری اصل مراقبت بایسته در فضای سایبر، می‌تواند راهگشا باشد، زیرا اثبات نقض تعهد مراقبت بایسته، نیازمند اثبات استاندارد بالای کنترل نیست و دولت‌ها را ملزم می‌کند که حداقل اقدامات معقول را برای جلوگیری از حملات سایبری از قلمرو خود انجام دهند. با این حال، اجرای این اصل نیز با چالش‌هایی مواجه است. از جمله مهم‌ترین این چالش‌ها، دشواری تعیین مصادیق عینی اقدامات معقول، تفاوت در توانایی‌های فنی و مالی دولت‌ها و نبود رویه قضایی مشخص در این زمینه است (لیو، ۲۰۱۷: ۲۰۰). سنجه سنجش مراقبت بایسته، یک سنجه عرفی و متغیر است که به توانایی‌های فنی و مالی دولت و همچنین جدیت تهدید بستگی دارد و از یک دولت توسعه‌یافته انتظار بیشتری نسبت به یک دولت درحال‌توسعه می‌رود (لیو، ۲۰۱۷: ۲۰۵). همچنین، این اصل عمدتاً در زمان صلح کاربرد دارد و در زمان مخاصمات مسلحانه، قواعد حقوق بشردوستانه بر آن مقدم خواهند بود (کولز، ۲۰۰۹:

فصلنامه طلوع نگارندگان عدالت
www.journaltne.ir

۱٤٥). با وجود این چالش‌ها، اصل مراقبت بایسته به‌عنوان یک راهکار عملی و متناسب با ویژگی‌های فضای سایبر، مورد توجه فزاینده جامعه بین‌الملل قرار گرفته است و انتظار می‌رود که در سال‌های آینده، نقش بیشتری در نظام حقوقی حاکم بر حملات سایبری ایفا کند.

۳- استانداردهای اثباتی در حملات سایبری

۳-۱.چالش‌های اثباتی در حوزه حملات سایبری

یکی از مهم‌ترین موانع در تحقق مسئولیت بین‌المللی دولت‌ها در قبال حملات سایبری، چالش‌های اثباتی است. بر خلاف حملات نظامی سنتی که آثار فیزیکی قابل‌مشاهده و مستند دارند، حملات سایبری اغلب اثری ناملموس از خود بر جای می‌گذارند و شناسایی عاملان آنها نیازمند تخصص فنی بالا و دسترسی به شواهد دیجیتال است (کولین، ۲۰۱۳: ٦۰). مهاجمان سایبری می‌توانند با استفاده از روش‌های پیشرفته، ردپای خود را پاک کنند و هرگونه ارتباط با خود را مخفی سازند. این ویژگی‌ها، اثبات انتساب یک حمله سایبری به یک دولت خاص را با دشواری‌های بی‌سابقه‌ای مواجه می‌سازد (بشیری، ۱۳۹٤: ۷).

چالش دیگر، تفاوت در استانداردهای اثباتی در نظام‌های حقوقی مختلف است. در حالی که برخی از دولت‌ها معیار «دلیل قاطع و روشن (Clear and Convincing Evidence) «را برای اثبات حملات سایبری طلب می‌کنند، برخی دیگر با معیار «موازنه احتمالات (Balance of Probabilities) «که سطح اثباتی پایین‌تری دارد، موافق هستند (امیری و حیدری‌فرد، ۱۳۹۷: ١٦٥). این عدم اجماع، به دولت‌ها امکان می‌دهد تا با بهره‌گیری از این ابهامات، از پذیرش مسئولیت خودداری کنند. همچنین، برخی از دولت‌ها معتقدند که اثبات حملات سایبری باید با استانداردهای کیفری انجام شود، در حالی که برخی دیگر معیارهای مدنی را کافی می‌دانند (اصلانی و رنجبریان، ۱۳۹٤: ٢٦٥). این تفاوت رویکردها، فرآیند اثبات را با پیچیدگی‌های بیشتری مواجه می‌سازد و هماهنگی بین‌المللی در این زمینه را دشوار می‌کند.

یکی دیگر از چالش‌های اثباتی، مسئله «جعل هویت (Spoofing) «در فضای سایبر است. مهاجمان می‌توانند آثاری از خود بر جای بگذارند که به‌طور عمدی به دولت دیگری نسبت داده شود و بدین‌ترتیب، فرآیند انتساب را با اشتباه مواجه کنند (کولین، ۲۰۱۳: ٦٨). این قابلیت، امکان انتساب اشتباه را افزایش می‌دهد و می‌تولند به تنش‌های بین‌المللی ناخواسته منجر شود. به‌عنوان مثال، در برخی از حملات سایبری، مهاجمان از آدرس‌های IP متعلق به کشورهای دیگر استفاده کرده‌اند تا این تصور را ایجاد کنند که حمله از آن کشورها صورت گرفته است، در حالی که مبدأ واقعی حمله جای دیگری بوده است. برای مقابله با این چالش‌ها، برخی از صاحبنظران بر ضرورت ایجاد یک نهاد تخصصی بین‌المللی با وظیفه بررسی فنی حملات سایبری و ارائه گزارش‌های کارشناسی تأکید کرده‌اند (نامدار و قاسمی، ۱۳۹۷: ۲۱۸).

۳-۲.رویه دولت‌ها در مواجهه با حملات سایبری به زیرساخت‌های حیاتی

فصلنامه طلوع نگارندگان عدالت
www.journaltne.ir

بررسی رویه دولت‌ها در مواجهه با حملات سایبری به زیرساخت‌های حیاتی، نشان‌دهنده نوعی سردرگمی و عدم اجماع در جامعه بین‌الملل است .بسیاری از دولت‌ها در موضع‌گیری‌های رسمی خود، بر اهمیت اصل مراقبت بایسته تأکید کرده‌اند، اما در عمل، به‌ندرت از این اصل برای طرح دعوی علیه دولت‌های دیگر استفاده می‌کنند (امیری و حیدری‌فرد، ۱۳۹۷: ۱۷۰). از یک سو، دولت قربانی با این دشواری مواجه است که اثبات نقض مراقبت بایسته، نیازمند افشای اطلاعات محرمانه مربوط به قابلیت‌های سایبری و روش‌های جمع‌آوری اطلاعات خود است و این امر، می‌تولند به امنیت ملی آن لطمه وارد کند. از سوی دیگر، دولت‌ها از این نگران هستند که پذیرش مسئولیت گسترده بر اساس اصل مراقبت بایسته، ممکن است به‌کارگیری گسترده‌ای از این اصل را علیه خودشان ممکن سازد و بدین‌ترتیب، دامنه مسئولیت‌پذیری آنان را بیش از حد افزایش دهد.

در مورد حملات سایبری به تأسیسات هسته‌ای ایران از طریق بدافزار استاکس‌نت، رژیم صهیونیستی و ایالات متحده از پذیرش رسمی مسئولیت خودداری کردند و به‌جای آن، راهبرد انکار معقول را در پیش گرفتند (نامدار و قاسمی، ۱۳۹۷: ۲۱۲). این رویکرد، نشان‌دهنده تمایل دولت‌ها به استفاده از فضای سایبر به‌عنوان عرصه‌ای برای اعمال راهبردهای خصمانه بدون پذیرش مسئولیت حقوقی است. حملات سایبری به زیرساخت‌های انرژی اوکراین در سال‌های اخیر نیز نمونه دیگری از این پدیده است که در آن، روسیه متهم به حملات سایبری به شبکه برق اوکراین شده است، اما این حملات به‌طور رسمی به دولت روسیه منتسب نشده است (کولز، ۲۰۰۹: ۱۴۸).

بررسی رویه دولت‌ها نشان می‌دهد که بسیاری از دولت‌ها به‌دلیل ملاحظات راهبردی و نگرانی از افشای اطلاعات محرمانه، تمایل چندانی به توسل به سازوکارهای حقوقی برای طرح دعوی علیه دولت‌های متخلف ندارند و ترجیح می‌دهند از طریق اقدامات متقابل سایبری پاسخ دهند. این رویکرد، هرچند عملاً کارآمد به نظر می‌رسد، اما از منظر حقوقی، نظام مسئولیت بین‌المللی را تضعیف می‌کند و نشان‌دهنده ناکارآمدی قواعد موجود در عمل است. همچنین، اقدامات متقابل سایبری می‌توانند به تشدید تنش‌ها و رویارویی نظامی منجر شوند و خطرات جدی برای صلح و امنیت بین‌المللی ایجاد کنند. از این رو، ضرورت تدوین قواعد روشن‌تر در زمینه حملات سایبری به زیرساخت‌های حیاتی و ایجاد سازوکارهای کارآمد برای حل‌وفصل اختلافات، بیش از پیش احساس می‌شود.

۳-۳.ضرورت تدوین استانداردهای اثباتی یکسان

با توجه به چالش‌های اثباتی موجود و عدم اجماع در جامعه بین‌الملل، ضرورت تدوین استانداردهای اثباتی یکسان در حوزه حملات سایبری به زیرساخت‌های حیاتی بیش از پیش احساس می‌شود. این استانداردها باید شامل معیارهای روشنی برای تشخیص حمله سایبری، تعیین سطح ادله مورد نیاز برای اثبات انتساب، و تعیین نقش شواهد فنی و اطلاعاتی در فرآیند اثبات باشد (اصلانی و رنجبریان، ۱۳۹٤: ۲۷۰). همچنین، این استانداردها باید به‌گونه‌ای تدوین شوند که هم از حاکمیت دولت‌ها حمایت کنند و هم پاسخگویی مؤثر در برابر حملات سایبری را تضمین نمایند.

فصلنامه طلوع نگارندگان عدالت
www.journaltne.ir

یکی از راهکارهای پیشنهادی در این زمینه، ایجاد یک «بانک اطلاعاتی بین‌المللی» از حملات سایبری است که در آن، اطلاعات مربوط به حملات سایبری، شواهد فنی و نتایج تحقیقات ثبت شود (محمدعلی‌پور، ۱۳۹۷: ۲۵۲). این بانک اطلاعاتی می‌تواند به دولت‌ها و مراجع قضـــایی در فرآیند اثبات کمک کند و از تکرار تحقیقات موازی جلوگیری نماید. همچنین، ایجاد یک «نهاد تخصـــصـــی بین‌المللی» با وظیفه بررســی فنی حملات ســایبری و ارائه گزارش‌های کارشـناسـی، می‌تواند به تسـهیل فرآیند اثبات و کاهش سـیاسـی‌شـدن آن کمک کند (نامدار و قاسـمی، ۱۳۹۷: ۲۱۸). این نهاد می‌تواند متشکل از کارشناسان مستقل و بی‌طرف از کشورهای مختلف باشد و به‌عنوان یک مرجع معتبر برای ارائه نظر کارشناسی در مورد مبدأ و ماهیت حملات سایبری عمل کند.

علاوه بر این، تدوین یک معاهده بین‌المللی در زمینه حملات سایبری به زیرساخت‌های حیاتی، می‌تواند چارچوب هنجاری روشـــنی برای تعیین مســـئولیت دولت‌ها فراهم آورد (لیو، ۲۰۱۷: ۲۱۰). این معاهده باید به‌صـــراحت، معیارهای انتساب را متناسب با ویژگی‌های فضای سایبر تعیین کند و تعهدات دولت‌ها را در زمینه مراقبت بایسته به‌صـــورت روشـــن‌تر تبیین نماید. با این حال، به دلیل اختلافات عمیق میان قدرت‌های بزرگ بر ســـر نحوه تنظیم فضـای سـایبر، پیشـرفت در این زمینه بسـیار کند بوده اسـت و انتظار نمی‌رود که در کوتاه‌مدت، توافقات جامعی در این زمینه حاصـــل شـــود (امیری و حیدری‌فرد، ۱۳۹۷: ۱۷۸). از این رو، در کنار تلاش برای تدوین معاهده جامع، می‌توان به توسعه قواعد عرفی و رویه قضایی در این زمینه نیز امید داشت.

٤- مطالعه موردی حملات سایبری به زیرساخت‌های حیاتی

٤-١.بدافزار استاکس‌نت؛ نقطه عطف حملات سایبری به زیرساخت‌های حیاتی

بدافزار اسـتاکس‌نت که در سـال ۲۰۱۰ شـناسـایی شـد، یکی از پیچیده‌ترین و پیشـرفته‌ترین حملات سـایبری تاریخ محسوب می‌شود که تأسیسات هسته‌ای ایران را هدف قرار داد. این بدافزار با حمله به سیستم‌های کنترلی صنعتی (SCADA)، موجب اختلال در عملکرد سـانتریفیوژها و تأخیر در برنامه هسـته‌ای ایران شـد (نامدار و قاسـمی، ۱۳۹۷: ۲۱۰). آنچه استاکس‌نت را از سایر حملات سایبری متمایز می‌ساخت، سطح بالای پیچیدگی فنی، استفاده از چندین آسیب‌پذیری روز صفر و هدف‌گیری دقیق و محدود بود که نشان می‌داد حملات با آگاهی کامل از جزئیات تأسیسات هدف طراحی شده‌اند (نامدار و قاسمی، ۱۳۹۷: ۲۱۲).

اسـتاکس‌نت از منظر حقوقی و سـیاسـی، تحولات گسـترده‌ای را در عرصـه جنگ سـایبری ایجاد کرد. نخسـت، این حمله نشان داد که حملات سایبری می‌توانند به‌اندازه حملات نظامی سنتی، خسارت‌بار و مؤثر باشند و از این رو، به عنوان یک ابزار راهبردی در منازعات بین‌المللی مورد توجه قرار گرفتند (محمدعلی‌پور، ۱۳۹۷: ۲٤۰). دوم، اسـتاکس‌نت مرزهای توسـل به زور در حقوق بین‌الملل را به چالش کشـید و این پرسـش را مطرح کرد که آیا یک حمله سـایبری که منجر به خسـارت فیزیکی می‌شـود، مصـداق «توسـل به زور» یا «حمله مسـلحانه» اسـت یا خیر (امیری و حیدری‌فرد، ۱۳۹۷: ۱٦۰). سوم، این حمله نشان داد که دولت‌ها می‌توانند با استفاده از ابزارهای سایبری،

فصلنامه طلوع نگارندگان عدالت
www.journaltne.ir

اهداف راهبردی خود را بدون توسل به جنگ نظامی مستقیم و بدون پذیرش مسئولیت رسمی، دنبال کنند (نامدار و قاسمی، ۱۳۹۷: ۲۱۵).

با این حال، استاکس‌نت چالش‌های حقوقی جدی را نیز در زمینه مسئولیت دولت‌ها ایجاد کرد. با توجه به اینکه رژیم صهیونیستی و ایالات متحده از پذیرش رسمی مسئولیت این حمله خودداری کردند، اثبات انتساب آن به یک دولت خاص با دشواری مواجه شد (نامدار و قاسمی، ۱۳۹۷: ۲۱۶). این موضوع، ناکارآمدی قواعد سنتی انتساب در فضای سایبر را به خوبی نشان داد و ضرورت تدوین قواعد جدید در این زمینه را آشکار ساخت. همچنین، استاکس‌نت این پرسش را مطرح کرد که آیا دولت ایران می‌توانسته است از حق دفاع مشروع در برابر این حمله استفاده کند یا خیر (امیری و حیدری‌فرد، ۱۳۹۷: ۱۶۳). پاسخ به این پرسش، مستلزم احراز اینکه آیا استاکس‌نت مصداق «حمله مسلحانه» بوده است یا خیر، می‌باشد که خود با اختلاف نظرهای جدی در جامعه بین‌الملل مواجه است.

٤-۲. حملات سایبری به زیرساخت‌های اوکراین و درس‌های آن

حملات سایبری به زیرساخت‌های اوکراین، به‌ویژه حملات به شبکه برق این کشور در سال‌های ۲۰۱۵ و ۲۰۱٦، نمونه دیگری از حملات سایبری به زیرساخت‌های حیاتی محسوب می‌شوند. این حملات که به روسیه منتسب شده‌اند، نشان دادند که زیرساخت‌های انرژی می‌توانند به‌راحتی هدف حملات سایبری قرار گیرند و اختلال در آنها می‌تواند پیامدهای گسترده‌ای برای جوامع داشته باشد (بشیری، ۱۳۹٤: ۵). در حمله سال ۲۰۱۵، هکرها با نفوذ به سیستم‌های کنترل شبکه برق اوکراین، توانستند برق حدود ۲۳۰ هزار نفر را برای چندین ساعت قطع کنند و این نخستین بار در تاریخ بود که یک حمله سایبری منجر به قطع گسترده برق می‌شد.

از منظر حقوقی، حملات سایبری به زیرساخت‌های اوکراین، چالش‌های متعددی را در زمینه مسئولیت بین‌المللی دولت‌ها ایجاد کردند. نخست، اثبات انتساب این حملات به روسیه با دشواری مواجه بود، زیرا هکرها از روش‌های پیشرفته پنهان‌سازی استفاده کرده بودند و ردپای خود را به‌خوبی پاک کرده بودند (کولین، ۲۰۱۳: ۷۰). دوم، حتی اگر انتساب اثبات می‌شد، تعیین اینکه آیا این حملات مصداق «توسل به زور» هستند یا خیر، محل اختلاف بود. برخی از صاحبنظران بر این باورند که حملات سایبری به زیرساخت‌های حیاتی که منجر به خسارت فیزیکی و اختلال در خدمات اساسی می‌شوند، می‌توانند مصداق توسل به زور تلقی شوند (امیری و حیدری‌فرد، ۱۳۹۷: ۱٦۵). سوم، پاسخ اوکراین به این حملات، محدود به اقدامات دیپلماتیک و ارتقای سطح امنیت سایبری خود بود و از توسل به اقدامات متقابل سایبری یا نظامی خودداری کرد که نشان‌دهنده محدودیت‌های عملی در پاسخ‌دهی به حملات سایبری است (حیدری‌فرد، ۱٤۰۰: ۱٦۸).

حملات سایبری به زیرساخت‌های اوکراین، درس‌های مهمی برای جامعه بین‌المللی داشت. نخست، آنها نشان دادند که زیرساخت‌های حیاتی کشورها به‌شدت در برابر حملات سایبری آسیب‌پذیر هستند و دولت‌ها باید سرمایه‌گذاری بیشتری در حوزه امنیت سایبری انجام دهند. دوم، این حملات نشان دادند که قواعد سنتی حقوق

فصلنامه طلوع نگارندگان عدالت
www.journaltne.ir

بین‌الملل برای پاسخگویی به چالش‌های ناشی از حملات سایبری کافی نیستند و ضرورت تدوین قواعد جدید و سازوکارهای کارآمد برای حل‌وفصل اختلافات در این زمینه بیش از پیش احساس می‌شود (محمدعلی‌پور، ۱۳۹۷: ۲۵۵). سوم، این حملات نشان دادند که اصل مراقبت بایسته، می‌تواند به عنوان مبنایی برای مسئولیت دولت‌ها در قبال حملات سایبری از قلمرو خود مورد استناد قرار گیرد (لیو، ۲۰۱۷: ۲۰۵). با این حال، اثبات نقض این اصل در عمل با دشواری‌های فراوانی مواجه است و نیازمند شواهد و مستندات قابل‌قبولی است.

٤-۳.حملات سایبری به زیرساخت‌های ایران؛ الگویی از تقابل سایبری نابرابر

جمهوری اسلامی ایران در سال‌های اخیر، هدف حملات سایبری متعددی قرار گرفته است که از جمله مهم‌ترین آنها می‌توان به حملات به تأسیسات هسته‌ای (استاکس‌نت)، حملات به سیستم‌های سوخت‌رسانی، حملات به تأسیسات بندری و حملات به سیستم‌های شهرداری و سازمان‌های دولتی اشاره کرد (بشیری، ۱۳۹٤: ۸). این حملات که عمدتاً به رژیم صهیونیستی و ایالات متحده منتسب می‌شوند، نشان‌دهنده الگویی از تقابل سایبری نابرابر هستند که در آن، یک طرف از برتری فنی قابل‌توجهی برخوردار است و از این برتری برای اعمال فشار بر طرف دیگر استفاده می‌کند (نامدار و قاسمی، ۱۳۹۷: ۲۲۰).

از منظر حقوقی، حملات سایبری به زیرساخت‌های ایران، چالش‌های متعددی را در زمینه مسئولیت بین‌المللی دولت‌ها ایجاد کرده است. نخست، اثبات انتساب این حملات به دولت‌های خاص با دشواری مواجه است، زیرا مهاجمان از روش‌های پیشرفته پنهان‌سازی استفاده می‌کنند و ردپای خود را به‌خوبی پاک می‌کنند (قرشی سروندانی، ۱۳۹۱: ۸۵). دوم، حتی اگر انتساب اثبات شود، تعیین اینکه آیا این حملات مصداق «توسل به زور» هستند یا خیر، محل اختلاف است. برخی از این حملات، مانند استاکس‌نت، به دلیل آثار مخرب فیزیکی، می‌توانند مصداق توسل به زور تلقی شوند، در حالی که برخی دیگر مانند حملات به سیستم‌های شهرداری، ممکن است در سطح مداخله باقی بمانند (امیری و حیدری‌فرد، ۱۳۹۷: ۱٦۸). سوم، ایران با محدودیت‌های جدی در زمینه پاسخگویی به این حملات مواجه است، زیرا عدم تقارن در قابلیت‌های سایبری، امکان پاسخ متقابل مؤثر را با دشواری مواجه می‌سازد (نامدار و قاسمی، ۱۳۹۷: ۲۲۲).

با وجود این محدودیت‌ها، ایران با تکیه بر راهبرد «بازدارندگی فعال» و «واکنش نامتقارن»، سعی کرده است تا حدی این عدم توازن را جبران کند و با نشان دادن توانایی خود در هدف‌گیری زیرساخت‌های حیاتی دشمن، هزینه‌های تهاجم سایبری را افزایش دهد (بشیری، ۱۳۹٤: ۱۰). با این حال، این راهبرد نیز با چالش‌های حقوقی متعددی مواجه است، از جمله اینکه پاسخ‌های سایبری ایران ممکن است خود ناقض قواعد حقوق بین‌الملل باشند و ایران را در معرض اتهامات حقوقی جدید قرار دهند. از این رو، به نظر می‌رسد که ایران نیز مانند سایر کشورها، نیازمند تدوین یک چارچوب حقوقی روشن‌تر برای مقابله با حملات سایبری به زیرساخت‌های حیاتی خود است و باید در این زمینه، هم‌چون سایر حوزه‌های حقوق بین‌الملل، به دنبال ایجاد قواعد شفاف و قابل‌پیش‌بینی باشد.

فصلنامه طلوع نگارندگان عدالت
www.journaltne.ir

نتیجه‌گیری

بررسی مسئولیت بین‌المللی دولت‌ها در قبال حملات سایبری به زیرساخت‌های حیاتی، ابعاد مختلف چالش‌های حقوقی ناشی از این نوع حملات را به تصویر کشیده است. یافته‌های پژوهش نشان می‌دهد که با وجود خلأ هنجاری موجود و عدم اجماع بر سر تعریف حمله سایبری و معیارهای انتساب، قواعد عمومی مسئولیت دولت‌ها و اصل مراقبت بایسته می‌توانند مبنایی برای مسئولیت دولت‌ها در قبال حملات سایبری از قلمرو خود فراهم آورند. با این حال، چالش‌های اثباتی، دشواری انتساب حملات به دولت‌ها و فقدان رویه قضایی مشخص، کاربست این قواعد را با دشواری مواجه ساخته است.

معیارهای کنترل مؤثر و کنترل کلی که در رویه قضایی بین‌المللی به رسمیت شناخته شده‌اند، برای فضای سایبر کارایی لازم را ندارند و اثبات انتساب حملات سایبری به دولت‌ها را با دشواری‌های بی‌سابقه‌ای مواجه می‌سازند. اصل مراقبت بایسته، هرچند می‌تواند راهکاری عملی‌تر ارائه دهد، اما اجرای آن با چالش‌هایی مانند دشواری تعیین مصادیق عینی اقدامات معقول و تفاوت در توانایی‌های فنی و مالی دولت‌ها مواجه است. همچنین، بررسی رویه دولت‌ها در مواردی مانند استاکس‌نت و حملات به زیرساخت‌های اوکراین و ایران نشان می‌دهد که دولت‌ها اغلب از پذیرش مسئولیت خودداری کرده و راهبرد انکار را در پیش می‌گیرند که این امر، پاسخ‌گویی در برابر حملات سایبری را با دشواری مواجه می‌سازد.

با توجه به یافته‌های این پژوهش، چند پیشنهاد برای ارتقای نظام حقوقی حاکم بر حملات سایبری به زیرساخت‌های حیاتی قابل ارائه است. نخست، ضرورت تدوین یک معاهده بین‌المللی خاص در زمینه حمایت از زیرساخت‌های حیاتی در برابر حملات سایبری که به‌صراحت، معیارهای انتساب را متناسب با ویژگی‌های فضای سایبر تعیین کند و تعهدات دولت‌ها را در زمینه مراقبت بایسته به‌صورت روشن‌تر تبیین نماید. دوم، ایجاد یک نهاد تخصصی بین‌المللی با وظیفه بررسی فنی حملات سایبری و ارائه گزارش‌های کارشناسی به دولت‌ها و مراجع قضایی، تا فرآیند انتساب فنی را تسهیل نماید و از سیاسی‌شدن آن جلوگیری کند. سوم، تدوین استانداردهای اثباتی یکسان و قابل‌قبول در جامعه بین‌الملل که معیارهای روشنی برای تشخیص حمله سایبری و تعیین سطح ادله مورد نیاز برای اثبات انتساب ارائه دهد. چهارم، توسعه همکاری‌های بین‌المللی در زمینه تبادل اطلاعات و تجارب در مورد نحوه مدیریت ریسک‌های سایبری و همچنین تدوین استانداردهای بین‌المللی برای اقدامات پیشگیرانه در فضای سایبر.

در نهایت، با توجه به اهمیت روزافزون فضای سایبر و افزایش تهدیدات متوجه زیرساخت‌های حیاتی، ضروری است که حقوق بین‌الملل با تحولات این حوزه همگام شود و چارچوب‌های هنجاری مناسبی برای پاسخگویی به چالش‌های نوین فراهم آورد. اگرچه در حال حاضر جامعه بین‌الملل در مورد معیارهای انتساب و نحوه اعمال قواعد مسئولیت دولت‌ها در فضای سایبر به اجماع کامل نرسیده است، اما روند رو به رشد حملات سایبری و

فصلنامه طلوع نگارندگان عدالت
www.journaltne.ir

افزایش آگاهی دولت‌ها از خطرات این حوزه، می‌تولند زمینه‌ساز تحولات مثبتی در آینده نزدیک باشد. انتظار می‌رود که رویه قضایی دولت‌ها، تلاش‌های نهادهای بین‌المللی و نیز همکاری‌های دوجانبه و چندجانبه در زمینه امنیت سایبری، گام‌های مؤثری در جهت پر کردن خلأهای موجود و ایجاد نظم حقوقی کارآمدتر در این عرصه بردارد. در غیر این صورت، ادامه وضعیت موجود، نه‌تنها به بی‌ثباتی در فضای سایبر دامن خواهد زد، بلکه می‌تواند به تشدید تنش‌های بین‌المللی و حتی رویارویی نظامی منجر شود که هزینه‌های جبران‌ناپذیری برای جامعه بین‌الملل به همراه خواهد داشت.

.

فهرست منابع

منابع فارسی

اصلانی، جبار و رنجبریان، امیرحسین. (۱۳۹٤). «بررسی تطبیقی و تحلیل تعریف حمله سایبری از منظر دکترین، رویه کشورها و سازمان‌های بین‌المللی در حقوق بین‌الملل». تحقیقات حقوقی، دوره ۱۸، شماره ۷۱، صص ۲۵۷-۲۷۸.

امیری، علی و حیدری‌فرد، مهدی. (۱۳۹۷). «جنگ‌های سایبری: چالش‌ها و راهکارهای تعامل در پرتو مقررات توسل به زور». سیاست خارجی، سال ۳۲، شماره ۳، صص ۱۵۳-۱۸۲.

بشیری، سپیده. (۱۳۹٤). «بررسی جایگاه حملات سایبری در حقوق بین‌الملل». پایان‌نامه کارشناسی ارشد، دانشگاه شهید بهشتی.

حلمی، نصرت‌الله (مترجم). (۱۳۸۷). مسئولیت بین‌المللی دولت و حمایت سیاسی. تهران: نشر میزان، چاپ اول.

حدادی، مهدی و مرادیان، بهرام. (۱۳۹۸). «مفهوم مراقبت بایسته در حقوق بین‌الملل و مقررات گروه ویژه اقدام مالی». مجله حقوق بین‌المللی، سال ۳٦، شماره ٦۱، صص ۱٦۵-۲۰۲.

حیدری‌فرد، مهدی. (۱٤۰۰). «اعمال مقررات حقوق بین‌الملل بشردوستانه در عرصه جنگ‌های سایبری: چالش‌ها و راهکارها». سیاست خارجی، سال ۳۵، شماره ٤، صص ۱۵۵-۱۷٤.

راعی، مسعود. (۱۳۸۸). «کنترل کلی یا مؤثر عاملی برای تحقق مسئولیت بین‌المللی دولت‌ها؟». مطالعات حقوق خصوصی، سال ۳۹، شماره ۳، صص ۱۵۱-۱٦٤.

ضیایی بیگدلی، محمدرضا. (۱۳۸٤). حقوق بین‌الملل عمومی. تهران: انتشارات گنج دانش، چاپ بیست‌ویکم.

قرشی سروندانی، سید هنرگس. (۱۳۹۱). مسئولیت بین‌المللی دولت‌ها در قبال حملات سایبری. پایان‌نامه کارشناسی ارشد، دانشکده حقوق دانشگاه شهید بهشتی.

ملکی‌زاده، امیرحسین. (۱۳۹۲). «ضابطه کنترل در نظام مسئولیت بین‌المللی؛ وحدت یا تعارض رویه قضایی بین‌المللی». مجله حقوقی دادگستری، سال ۷۷، شماره ۸۲، صص ۱٦۰-۱۹۱.

فصلنامه طلوع نگارندگان عدالت
www.journaltne.ir

محمدعلی‌پور، فریده. (۱۳۹۷). «حملات سایبری و چالش‌های جدید برای اصل منع توسل به زور در روابط بین‌الملل». مطالعات حقوقی، سال ٦، شماره ۳، صص ۲۳۳-۲۵۷.

نامدار، ساسان و قاسمی، غلامعلی. (۱۳۹۷). «تحلیل مفهوم دفاع مشروع در پرتو حملات سایبری (با تأکید بر حمله استاکس‌نت به تأسیسات هسته‌ای ایران)». مطالعات حقوق عمومی، سال ٤٨، شماره ٤، صص ۱۹۹-۲۳۵.

نصیری محلاتی، ژوبین. (۱۳۸۹). بررسی انطباق تصمیمات محاکم آمریکا در انتساب اعمال افراد و گروه‌ها به دولت ایران. پایان‌نامه کارشناسی ارشد، دانشگاه شهید بهشتی.

منابع خارجی

Collin, S. A. (۲۰۱۳). Attribution issues in cyberspace. *Chicago-Kent Journal of International and Comparative Law*, ۱۳(۲), ۵۷-۸۲.

International Court of Justice. (۱۹٤۹). *The Corfu Channel Case (United Kingdom v. Albania) (Merits)*. Judgment of ۹ April ۱۹٤۹. I.C.J. Reports ۱۹٤۹.

International Court of Justice. (۱۹۸٦). *Military and para-military activities in and against Nicaragua (Nicaragua v. United States of America) (Merits)*. Judgment of ۲۷ June ۱۹۸٦. I.C.J. Reports ۱۹۸٦.

International Court of Justice. (۱۹۹٦). *Legality of the threat or use of nuclear weapons*. Advisory Opinion of ۸ July ۱۹۹٦. I.C.J. Reports ۱۹۹٦.

International Court of Justice. (۲۰۰۳). *Oil platforms (Islamic Republic of Iran v. United States of America)*. Judgment of ٦ November ۲۰۰۳. I.C.J. Reports ۲۰۰۳.

International Court of Justice. (۲۰۰٤). *Legal consequences of the construction of a wall in the occupied Palestinian territory*. Advisory Opinion of ۹ July ۲۰۰٤. I.C.J. Reports ۲۰۰٤.

International Court of Justice. (۲۰۰۷). *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)*. Judgment of ۲٦ February ۲۰۰۷. I.C.J. Reports ۲۰۰۷.

International Law Commission. (۲۰۰۱). *Draft Articles on Responsibility of States for Internationally Wrongful Acts*. UN Doc. A/٥٦/۱۰.

Kulesza, J. (۲۰۰۹). State Responsibility for Cyberattacks on International Peace and Security. *Polish Yearbook of International Law*, (۲۹), ۱۳۹-۱٥۲.

Liu, I. Y. (۲۰۱۷). State Responsibility and Cyberattacks: Defining Due Diligence Obligations. *The Indonesian Journal of International and Comparative Law*, ٤, ۱۹۱-۲۲۰.

Schmitt, M. N. (Ed.). (۲۰۱۳). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge University Press.